Boolean Lattice

A Boolean lattice is a relation satisfying a long list of conditions. This can be decomposed into the following ascending chain of definitions.

Definition. A *preorder*[1] is a relation $\leq$ that is reflexive and transitive.

A *partial order* is a preorder $\leq$ that is antisymmetric, i.e $x \leq y \leq x$ implies $x = y$.

A *lattice* is a partial order in which every pair of elements x, y have a meet $x \wedge y := \inf\{x, y\}$ and a join $x \vee y := \sup\{x, y\}$. A *bounded* lattice is a lattice which has a minimum $\hat{0}$ and a maximum $\hat{1}$.

A *distributive lattice* is a lattice D in which

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

and

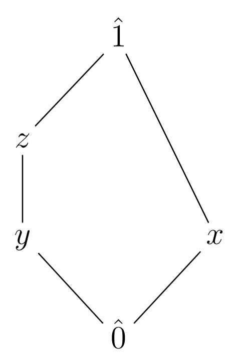
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

for all $x, y, z \in D$.

A *complement* of an element x of a bounded lattice L is an $x' \in L$ such that $x \wedge x' = \hat{0}$ and $x \vee x' = \hat{1}$. A *Boolean lattice* is a bounded distributive lattice in which every element has a unique complement.

Example. Taking the power set of a set X yields a Boolean lattice $(2^X, \subseteq)$. Meets are intersections, joins are unions, and the complement of a $Y \subseteq X$ is $X \setminus Y$.

Example. The lattice N_5 is given below.



Here,

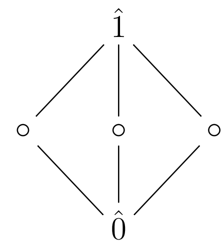
$$x \wedge y = \hat{0} = x \wedge z$$

and

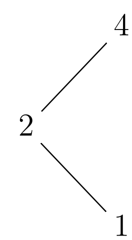
$$x \vee y = \hat{1} = x \vee z\,,$$

so y, z are both complements of x.

Example. The lattice M_3 is given below.



A lattice is distributive if and only if it has no sublattices isomorphic to N_5 or M_3. So, the lattice below is distributive.



But, this lattice is not Boolean since 2 has no complement. More generally, it is possible to show that the distributive lattice of positive divisors of an $n \in \mathbb{Z}^+$ ordered by divisibility is Boolean if and only if n is squarefree.

Example. The two-element lattice $\{0, 1\}$ with $0 < 1$ is Boolean. The complement of a $x \in \{0, 1\}$ is $1 - x$.

The chain at the beginning of this section also has two branches we will use.

Definition. An *equivalence relation* is a preorder $\equiv$ that is symmetric, i.e. $x \equiv y$ implies $y \equiv x$.

A *linear order* is a partial order $\leq$ such that every pair of elements x, y are comparable, i.e. $x \leq y$ or $y \leq x$.

[1] Equivalently, a preorder is a category in which, for each pair of objects x, y, there is at most one morphism from x to y. Then, meets are products and joins are coproducts.

Formulas

For each set A, we can construct the set W_A of well-formed formulas on A as follows. Let A be a set which is arbitrary unless otherwise specified.

Let $C = \{\neg, \vee, \wedge, \rightarrow, (,)\}$ be a set of 6 currently meaningless symbols. Let S be the set of strings on $A \cup C$. Define maps $\varepsilon_\neg : S \to S$ and $\varepsilon_\vee, \varepsilon_\wedge, \varepsilon_\rightarrow : S \times S \to S$ by

$$\begin{aligned} \varepsilon_\neg(\psi) &= \neg(\psi) \\ \varepsilon_\vee(\phi, \psi) &= (\phi \vee \psi) \\ \varepsilon_\wedge(\phi, \psi) &= (\phi \wedge \psi) \\ \varepsilon_\rightarrow(\phi, \psi) &= (\phi \rightarrow \psi) \end{aligned}$$

for all $\phi, \psi \in S$. Inductively define subsets W_i of S for $i \in \mathbb{Z}^+$ as follows. Let $W_1 = A$. If $i \in \mathbb{Z}^+$ such that W_i has been defined, set

$$W_{i+1} = W_i \cup \varepsilon_\neg(W_i) \cup \bigcup_{\oplus \in \{\vee, \wedge, \rightarrow\}} \varepsilon_\oplus(W_i \times W_i)\,.$$

Let $W_A = \bigcup_{i \in \mathbb{Z}^+} W_i$. The elements of A will be called *atoms*, and the elements of W_A will be called *well-formed formulas*. Elements of $S \setminus W_A$ such as $\rightarrow)((\wedge\neg$ are indeed ill-formed. Next, we see how to assign some meaning to the elements of W_A.

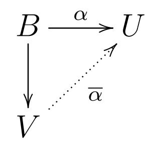
Definition. A map $v : W_A \to \{0, 1\}$ is a *valuation* if and only if

$$\begin{aligned} v(\neg\phi) &= 1 - v(\phi) \\ v(\phi \vee \psi) &= \max\{v(\phi), v(\psi)\} \\ v(\phi \wedge \psi) &= \min\{v(\phi), v(\psi)\} \\ v(\phi \rightarrow \psi) &= \max\{1 - v(\phi), v(\psi)\} \end{aligned}$$

for all $\phi, \psi \in W_A$.

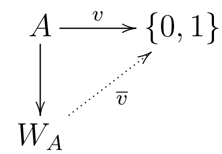
So, a valuation is a map which assigns a truth-value to each well-formed formula in a way that respects the connectives.

Recall that vector spaces are free over their bases. If V is a vector space with basis B, and U is another vector space, then any map $\alpha : B \to U$ can be uniquely extended to a linear map $\overline{\alpha} : V \to U$.



Similarly, the set of well-formed formulas W_A is free over the atoms A.

Proposition. Suppose $v : A \to \{0, 1\}$ is a map. Then, there exists a unique valuation $\overline{v} : W_A \to \{0, 1\}$ such that $\overline{v}(a) = v(a)$ for all $a \in A$.



Now, let's see an example of how well-formed formulas can be used to express useful things. Let P be a set. We have the following bijective correspondence between the relations on P and the valuations $W_{P \times P} \to \{0, 1\}$. Using the previous proposition, for each relation $\sim$ on P, we can let $v_\sim : W_{P \times P} \to \{0, 1\}$ be the valuation with $v_\sim((y, z)) = 1$ if and only if $y \sim z$. Then

$$\sim \mapsto v_\sim$$

is a bijection from the set of relations on P to the set of valuations $W_{P \times P} \to \{0, 1\}$. If relations on P are viewed as subsets of $P \times P$, then the inverse bijection is

$$v \mapsto v^{-1}(\{1\}) \cap X \times X\,.$$

Observe that a relation $\sim$ on P is reflexive if and only if

$$1 = v_\sim((p, p))$$

for all $p \in P$. A relation $\sim$ on P is transitive if and only if

$$1 = v_\sim(((p, q) \wedge (q, r)) \rightarrow (p, r))$$

for all $p, q, r \in P$. Indeed, if $p, q, r \in P$ with $p \sim q$ and $q \sim r$ and

$$1 = v_\sim(((p, q) \wedge (q, r)) \rightarrow (p, r))\,,$$

then $v(p,q) = v(q,r) = 1$ and

$$\begin{aligned} 1 &= \max\{1 - \min\{v(p,q), v(q,r)\}, v(p,r)\} \\ &= \max\{0, v(p,r)\}\,, \end{aligned}$$

whence $v(p,r) = 1$ and $p \sim r$. If $\sim$ is transitive and $p,q,r \in P$ and $v(p,r) = 0$, then $v(p,q) = 0$ or $v(q,r) = 0$, so

$$\begin{aligned} &v_\sim(((p,q) \wedge (q,r)) \to (p,r)) \\ &\quad = \max\{1 - \min\{v(p,q), v(q,r)\}, 0\} \\ &\quad = 1 - \min\{v(p,q), v(q,r)\} \\ &\quad = 1\,. \end{aligned}$$

Similarly for antisymmetry and comparability. Let

$$\begin{aligned} T =& \{(p,q) \in P \times P \mid p = q\} \\ &\cup \{((p,q) \wedge (q,r)) \to (p,r) \mid p,q,r \in P\} \\ &\cup \{\neg((p,q) \wedge (q,p)) \mid p,q \in P \text{ and } p \neq q\} \\ &\cup \{(p,q) \vee (q,p) \mid p,q \in P\}\,. \end{aligned}$$

So, a relation $\sim$ on P is a linear order if and only if $1 = \inf v_\sim(T)$.

Preorder to Partial Order

The following is a natural[2] way to obtain a partial order from a preorder. Suppose $\leq$ is a preorder on a set X. Define an equivalence relation $\equiv$ on X by $x \equiv y$ if and only if $x \leq y$ and $y \leq x$. For each $x \in X$, let

$$[x] = \{y \in X \mid y \equiv x\}$$

denote the equivalence class of x. Let

$$X^* = (X/\equiv) = \{[x] \mid x \in X\}$$

denote the quotient of X by $\equiv$. Define the relation $\leq^*$ on X^* by $[x] \leq^* [y]$ if and only if $x \leq y$.

Proposition. The relation $\equiv$ is indeed an equivalence relation. The relation $\leq^*$ is a well-defined partial order.

Proof. The relation $\equiv$ is reflexive and transitive since $\leq$ is reflexive and transitive. The relation $\equiv$ is symmetric since its definition is symmetric.

If $a \equiv y \leq z \equiv b$, then $a \leq y \leq z \leq b$ and $a \leq b$. The relation $\leq^*$ is a partial order since $\leq$ is a partial order. □

Define a relation $\vDash$ on W_A by $\phi \vDash \psi$ if and only if $v(\phi) \leq v(\psi)$ for all valuations v. Equivalently, $\phi \vDash \psi$ if and only if, for all valuations v, we have $v(\phi) = 1$ implies $v(\psi) = 1$.

Proposition. The relation $\vDash$ is a preorder.

Proof. Suppose $\phi \in W_A$. Since $v(\phi) \leq v(\phi)$ for all valuations v, we have $\phi \vDash \phi$.

Suppose $\phi, \psi, \chi \in W_A$ with $\phi \vDash \psi$ and $\psi \vDash \chi$. If v is a valuation, then $v(\phi) \leq v(\psi)$ and $v(\psi) \leq v(\chi)$, and thus $v(\phi) \leq v(\chi)$. So $\phi \vDash \chi$. □

So, we have a partial order $\vDash^*$ with $\phi \vDash \psi$ if and only if $[\phi] \vDash^* [\psi]$. Note that $v(\phi) = v(\psi)$ for all valuations v if and only if $[\phi] = [\psi]$.

Proposition. The partial order $\vDash^*$ is a Boolean lattice.

Proof. Suppose $[\phi], [\psi] \in W_A^*$. For all valuations v, we have

$$v(\phi) \leq \max\{v(\phi), v(\psi)\} = v(\phi \vee \psi)\,,$$

so $\phi \vDash \phi \vee \psi$. Hence $[\phi] \vDash^* [\phi \vee \psi]$. Similarly, $[\psi] \vDash^* [\phi \vee \psi]$. So $[\phi \vee \psi]$ is a common upper bound for $[\phi]$ and $[\psi]$.

Suppose $[\chi] \in W_A^*$ is another common upper bound for $[\phi]$ and $[\psi]$. Then, for all valuations v, we have $v(\phi) \leq v(\chi)$ and $v(\psi) \leq v(\chi)$, so

$$v(\phi \vee \psi) = \max\{v(\phi), v(\psi)\} \leq v(\chi)\,.$$

[2] This way of turning preorders into partial orders is functorial, and is left adjoint to the forgetful functor from the category of partial orders to the category of preorders.

Hence $\phi \vee \psi \vDash \chi$, i.e. $[\phi \vee \psi] \vDash^* [\chi]$.

So, $[\phi \vee \psi]$ is the least upper bound of $[\phi]$ and $[\psi]$, i.e.

$$[\phi] \vee [\psi] = [\phi \vee \psi] .$$

Similarly,

$$[\phi] \wedge [\psi] = [\phi \wedge \psi] .$$

So, $\vDash^*$ is a lattice. Also, this shows that it makes sense to use the same symbols for disjunction and conjunction for logic as for join and meet for orders.

A *tautology* is a $\phi \in W_A$ such that $v(\phi) = 1$ for all valuations v. Pick an $a \in W_A$ and set $\top = (a \vee (\neg a))$. For all valuations v, we have

$$\begin{aligned} v(\top) &= v(a \vee (\neg a)) \\ &= \max\{v(a), v(\neg a)\} \\ &= \max\{v(a), 1 - v(a)\} \\ &= 1 \end{aligned}$$

So, for all $\phi \in W_A$, we have

$$v(\phi) \leq 1 = v(\top)$$

for all valuations v, and thus $\phi \vDash \top$, i.e. $[\phi] \vDash^* [\top]$. So, $[\top]$ is the maximum element of W_A^*.

A *contradiction* is a $\phi \in W_A$ such that $v(\phi) = 0$ for all valuations v. Pick an $a \in W_A$, set $\perp = (a \wedge (\neg a))$, and observe that similarly $\perp$ is a contradiction and hence $[\perp]$ is the minimum element of W_A^*.

Suppose $[\phi] \in W_A^*$. For all valuations v, we have

$$\begin{aligned} v(\phi \vee (\neg \phi)) &= \max\{v(\phi), v(\neg \phi)\} \\ &= \max\{v(\phi), 1 - v(\phi)\} \\ &= 1 \\ &= v(\top) . \end{aligned}$$

It follows that

$$[\phi] \vee [\neg \phi] = [\phi \vee (\neg \phi)] = [\top] ,$$

Similarly,

$$[\phi] \wedge [\neg \phi] = [\perp] .$$

So $[\neg \phi]$ is a complement of $[\phi]$. Suppose $[\psi] \in W^*$ is another complement of $[\phi]$. Then

$$[\phi \vee \psi] = [\phi] \vee [\psi] = [\top] .$$

Suppose v is a valuation. Then

$$\begin{aligned} 1 &= v(\top) \\ &= v(\phi \vee \psi) \\ &= \max\{w(\phi), w(\psi)\} . \end{aligned}$$

If $v(\phi) = 0$, then this implies

$$v(\psi) = 1 = 1 - 0 = v(\neg \phi) .$$

Otherwise, if $v(\phi) = 1$, consider instead

$$\begin{aligned} 0 &= v(\perp) \\ &= v(\phi \wedge \psi) \\ &= \min\{v(\phi), v(\psi)\} , \end{aligned}$$

whence

$$v(\psi) = 0 = 1 - 1 = v(\neg \phi) .$$

So $v(\psi) = v(\neg \phi)$ for all valuations v, i.e. $[\psi] = [\neg \phi]$. So, the complement of $[\phi]$ is unique. $\square$

We now have a counterexample to the infinite extension of the following theorem.

Theorem. Each finite Boolean lattice is isomorphic to $(2^{[n]}, \subseteq)$ for some $n \in \mathbb{Z}^+ \cup \{0\}$.

Recall that Cantor's Theorem says that if X is a set, then there are no injections $2^X \to X$. In particular, the powerset of a set is either finite or uncountable. If A is chosen to be countably infinite, then the Boolean lattice W_A^* is countably infinite and hence not isomorphic to a powerset lattice.

Partial Order to Linear Order

Definition. A subset $S \subseteq W_A$ is *satisfiable* if and only if there exists a valuation v such that $\inf v(S) = 1$, i.e. such that $v(\phi) = 1$ for all $\phi \in S$.

Example. Suppose $a \in A$. Then $\{a, (\neg a)\}$ is not satisfiable since, if v is a valuation with $v(a) = 1$, then $v(\neg a) = 1 - 1 = 0 \neq 1$.

Theorem. A subset $S \subseteq W$ is satisfiable if and only if every finite subset of S is satisfiable.

The theorem above is the Compactness Theorem.[3] It can be used to extend various results to the infinite case. Dilworth's Theorem for partial orders of finite width is one example. Another is the following.

Definition. A *linear extension* of a partial order $\preceq$ on a set P is a linear order $\leq$ on P such that $p \preceq q$ implies $p \leq q$. If relations on P are viewed as subsets of $P \times P$, then this is the same as saying $\preceq \subseteq \leq$.

Lemma. Every finite partial order has a linear extension.

Proof. Suppose $(P, \preceq)$ is a partial order, and $y, z \in P$ are incomparable. Define a relation $\leq$ on P by $p \leq q$ if and only if $p \preceq q$, or $p \preceq y$ and $q \preceq z$. So, $\leq$ is an extension of $\preceq$ having fewer pairs of incomparable elements than $\preceq$. Observe that it is possible to use the fact that $\preceq$ is a partial order to check that $\leq$ is a partial order. So, induction can be used to obtain the desired result. □

Proposition. Every partial order has a linear extension.

Proof. Suppose $(P, \preceq)$ is a partial order. Let

$$S_e = \{(p, q) \in P \times P \mid p \preceq q\}$$
$$S_t = \{((p, q) \wedge (q, r)) \to (p, r) \mid p, q, r \in P\}$$
$$S_a = \{\neg((p, q) \wedge (q, p)) \mid p, q \in P \text{ and } p \neq q\}$$
$$S_c = \{(p, q) \vee (q, p) \mid p, q \in P\}\,.$$

Let

$$S = S_e \cup S_t \cup S_a \cup S_c \subseteq W_{P \times P}\,.$$

Suppose $F \subseteq S$ is finite. Let $Q \subseteq P$ be the set of consisting of all elements of P appearing in F. Then Q is finite since F is finite and the elements of F are finite strings. Then Q is a finite subposet of P, so the lemma yields a linear extension $\leq$ of the ordering on Q induced by $\preceq$. Let $v : W_{Q \times Q} \to \{0, 1\}$ be the valuation with $v(r, s) = 1$ for $r \leq s$ and $v(r, s) = 0$ for $r \not\leq s$.

Suppose $(p, q) \in S_e \cap F$. Then $p \preceq q$ and $p, q \in Q$. Since $p \preceq q$ and $\leq$ is an extension of $\preceq$, we have $p \leq q$. Then $v(p, q) = 1$. Similarly, since $\leq$ is transitive, antisymmetric, and has comparability, it is possible to show that $v(\phi) = 1$ for all $\phi \in (S_t \cup S_a \cup S_c) \cap F$.

It follows that F is satisfiable. Using the Compactness Theorem, there exists a valuation $v : W_{P \times P} \to \{0, 1\}$ such that $v(\phi) = 1$ for all $\phi \in S$. Using the last paragraph of the second section, the relation $\leq$ on P given by

$$p \leq q \quad \text{if and only if} \quad v(p, q) = 1$$

for all $p, q \in P$ is a linear extension of $\preceq$. □

Video

youtu.be/f3a-o-Vn7Fg

References

[1] B.A. Davey and H.A. Priestly, *Introduction to Lattices and Order*, first edition

[2] J.B. Nation, *Notes on Lattice Theory.* math.hawaii.edu/~jb/math618/Nation-LatticeTheory.pdf

[3] P. Johnstone, *Notes on Logic and Set Theory*

[3] The name of this theorem makes sense since it can be proved using Tychnoff's theorem.